PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-044353
(43)Date of publication of application : 14.02.1997

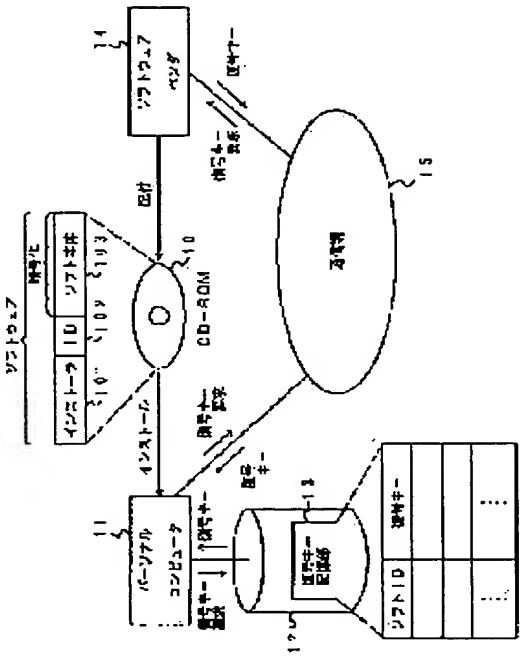
(51)Int.Cl. G06F 9/06
G06F 9/06
G06F 15/00
G09C 1/00
G09C 1/00

(21)Application number : 07-194695
(22)Date of filing : 31.07.1995

(71)Applicant : TOSHIBA CORP
(72)Inventor : YOSHIDA HIDEKI
SEGAWA HIDEO
IMAI TORU

(54) DECODING KEY MANAGEMENT METHOD, COMPUTER ADOPTING THE METHOD, AND SOFTWARE METHOD AND SYSTEM USING THE KEY

(57)Abstract:
PROBLEM TO BE SOLVED: To improve the reliability or a software distribution system using a cipher by increasing the number of degrees of freedom of erasing and re- installation of ciphered software.
SOLUTION: A decoding key to decode a ciphered software main body 103 is preserved in a decoding key storage part 13 correspondingly to the software ID. An installer 101 retrieves the decoding key storage part 13; and if the pertinent decoding key is not found, the decoding key is obtained from a software vendor 104 by communication with this vendor 104. After this decoding key is stored in the decoding key storage part 13 corresponding to the software ID, the software main body 103 is decoded and is installed to a hard disk device 12. Since the key is reused at the time of decoding the software main body 103 again, it is unnecessary for a user to get the decoding key from the vendor 14 plural times.



LEGAL STATUS

[Date of request for examination] 14.09.2000
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3507594
[Date of registration] 26.12.2003
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－44353

(43)公開日　平成９年(1997)２月14日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	9/06	５５０		Ｇ０６Ｆ	9/06	５５０Ａ
		４１０				４１０Ｂ
	15/00	３３０	9364－5L		15/00	３３０Ｚ
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｂ
		６６０	7259－5Ｊ			６６０Ｄ

審査請求　未請求　請求項の数６　ＯＬ　（全 12 頁）

(21)出願番号　特願平7－194695

(22)出願日　平成７年(1995)７月31日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　吉田　英樹
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　瀬川　英生
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　今井　徹
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

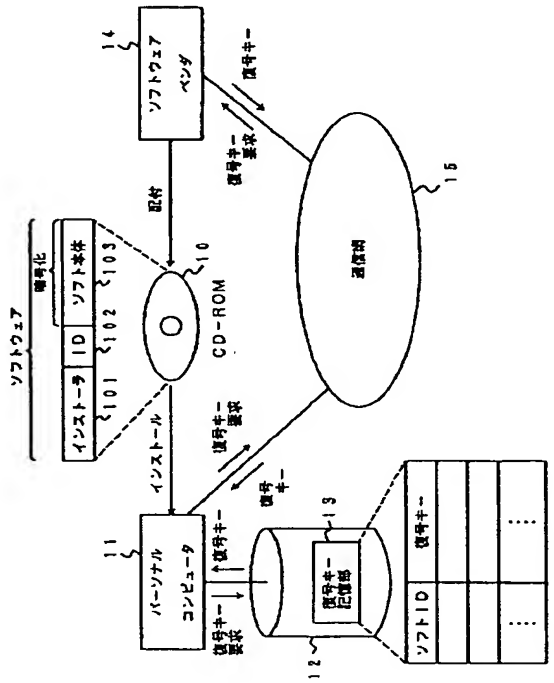
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　復号鍵管理方法およびその方法が適用されるコンピュータ、並びに復号鍵を使用したソフトウェア流通方法および流通システム

(57)【要約】

【課題】暗号化ソフトウェアの消去および再インストールを自由度を高め、暗号を利用したソフトウェア流通システムの信頼性の向上を図る。

【解決手段】復号キー記憶部１３には、暗号化されたソフトウェア本体１０３を復号化するための復号キーがソフトウェアＩＤと対応付けられて保存されている。インストーラ１０１は、復号キー記憶部１３を検索し、該当する復号キーがないならば、ソフトウェアベンダ１０４と通信して、ソフトウェアベンダ１０４から復号キーを入手する。そして、その復号キーをソフトウェアＩＤと対応付けて復号キー記憶部１３に保存した後、ソフトウェア本体１０３の復号化およびハードディスク装置１２へのインストールを行う。よって、次回にそのソフトウェア本体１０３を再び復号化する際にはそのキーが再利用されるため、利用者は復号キーを複数回ベンダ１４から入手せずに済む。



1

【特許請求の範囲】
【請求項１】　暗号化されたソフトウェアを導入すべきコンピュータの記憶装置から前記ソフトウェアを解読するための復号鍵を検索し、
前記復号鍵を検索できたとき、その復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、
前記復号鍵を検索できなかったとき、前記暗号化されたソフトウェアの配布元から、前記ソフトウェアに対応する復号鍵を入手するための手続きを実行し、
その入手した復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入すると共に、その復号鍵を前記ソフトウェアと別個に前記コンピュータの記憶装置内に保存し、
前記暗号化されたソフトウェアの再導入のときは前記記憶装置内に保存されている復号鍵を利用して前記ソフトウェアを復号化できるようにしたことを特徴とするソフトウェア復号鍵管理方法。
【請求項２】　暗号化された複数のソフトウェアをインストール可能なコンピュータであって、
ソフトウェア識別情報とそのソフトウェアを解読するための復号鍵とを対応付けて格納するための復号鍵記憶手段と、
導入対象の暗号化されたソフトウェアからソフトウェア識別情報を取得し、そのソフトウェア識別情報を利用して、前記暗号化されたソフトウェアを解読するための復号鍵を前記復号鍵記憶手段から検索する復号鍵検索手段と、
この復号鍵検索手段によって前記復号鍵を検索できたとき、その復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入する手段と、
前記復号鍵を検索できなかったとき、前記暗号化されたソフトウェアの配布元から前記ソフトウェアに対応する復号鍵を通信網を介して入手するための通信手続きを実行する復号鍵入手手段と、
この復号鍵入手手段によって入手された復号鍵を、前記導入対象の暗号化されたソフトウェアを特定するための識別情報と対応付けて前記復号鍵記憶手段に保存する手段と、
前記入手された復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入する手段とを具備することを特徴とするコンピュータ。
【請求項３】　少なくとも１つの暗号化されたソフトウェア本体と、復号鍵を利用して前記ソフトウェア本体を復号化するための復号化プログラムとを含むソフトウェアを、記録媒体または通信媒体を介して流通させるソフトウェア流通方法であって、
前記復号化プログラムを、前記ソフトウェア本体を導入すべきコンピュータに実行させることによって、
前記コンピュータの記憶装置内から前記ソフトウェア本体を解読するための復号鍵を検索し、
前記復号鍵を検索できたとき、その復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、
前記復号鍵を検索できなかったとき、前記暗号化されたソフトウェアの配布元から、前記ソフトウェアに対応する復号鍵を入手するための手続きを実行し、
その入手した復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、その復号鍵を前記ソフトウェアと別個に前記コンピュータの記憶装置内に保存することを特徴とするソフトウェア流通方法。
【請求項４】　暗号化されたソフトウェアを配布し、使用料の支払いと引き替えに前記暗号化されたソフトウェアを復号化するための復号鍵を発行するソフトウェア流通方法で使用される記録媒体であって、
この記録媒体には、少なくとも１つの暗号化されたソフトウェア本体と、復号鍵を利用して前記ソフトウェア本体を復号化するための復号化プログラムとが含まれ、
前記復号化プログラムには、暗号化されたソフトウェアを導入すべきコンピュータの記憶装置から前記ソフトウェアを解読するための復号鍵を検索し、
前記復号鍵を検索できたとき、その復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、
前記復号鍵を検索できなかったとき、前記暗号化されたソフトウェアの配布元から、前記ソフトウェアに対応する復号鍵を入手するための手続きを実行し、
その入手した復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、その復号鍵を前記ソフトウェアと別個に前記コンピュータの記憶装置内に保存する手続きが記述されていることを特徴とする記録媒体。
【請求項５】　暗号化されてユーザに配布されるソフトウェアそれぞれを解読するめための復号鍵を保持する計算機センタと、この計算機センタから復号鍵を入手してソフトウェアを復号化するユーザ端末とを接続可能な通信網を利用して、ソフトウェアを流通させるソフトウェア流通システムにおいて、
前記ユーザ端末は、
ソフトウェア識別情報とそのソフトウェアを解読するための復号鍵とを対応付けて格納するための復号鍵記憶手段と、
導入対象の暗号化されたソフトウェアを解読するための復号鍵を、前記復号鍵記憶手段から検索する復号鍵検索手段と、
この復号鍵検索手段によって前記復号鍵を検索できたとき、その復号鍵を利用して前記暗号化されたソフトウェ

アを復号化して前記ユーザ端末に導入する手段と、
前記復号鍵を検索できなかったとき、前記計算機センタに復号鍵を要求する事によって、前記ソフトウェアに対応する復号鍵を前記計算機センタから通信網を介して入手する復号鍵入手手段と、
この復号鍵入手手段によって入手された復号鍵を、前記導入対象の暗号化されたソフトウェアを特定するための識別情報と対応付けて前記復号鍵記憶手段に保存する手段と、
前記入手された復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記ユーザ端末に導入する手段とを具備し、
前記計算機センタは、
前記ユーザ端末からの復号鍵要求に応答して、ソフトウェア使用量を課金するための情報を生成する手段と、
前記復号鍵要求に応答して、復号鍵をユーザ端末に送信する手段とを具備することを特徴とするソフトウェア流通システム。
【請求項６】　暗号化されたソフトウェアを導入すべきコンピュータの記憶装置から前記ソフトウェアを解読するための復号鍵を検索し、
前記復号鍵を検索できたとき、その復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、
前記復号鍵を検索できなかったとき、前記暗号化されたソフトウェアの配布元から前記ソフトウェアに対応する復号鍵を入手し、その入手した復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、
前記ソフトウェアを前記コンピュータの記憶装置から消去するとき、前記復号鍵を前記記憶装置に保存し、
前記暗号化されたソフトウェアの再導入のときは前記記憶装置内に保存されている復号鍵を利用して前記ソフトウェアを復号化できるようにしたことを特徴とするソフトウェア復号鍵管理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、暗号化されたソフトウェアを復号化するための鍵（キー）の管理方法およびその方法が適用されるコンピュータ、並びに復号鍵を使用したソフトウェア流通方法および流通システムに関する。
【０００２】
【従来の技術】従来、コンピュータで使用されるソフトウェアは、それぞれ個別にフロッピーディスクなどの記憶媒体に格納され、マニュアルなどとともにパッケージに封入された状態で小売店で販売されるのが通常の販売形態であった。
【０００３】このようなパッケージソフトウェアの場合、ソフトウェアの利用許諾などを行なうライセンシング

は、ソフトウェアのパッケージの販売と不可分の形で行なわれるのが一般的である。たとえば、パッケージを開封した時点でソフトウェアの利用契約が成立する旨が記述された文書がソフトウェアに付随して配布される場合や、パッケージに付属の利用者登録葉書をただちに記入してベンダと利用契約を結ぶことが求められる場合が多い。
【０００４】これに対し、最近では、従来のようにソフトウェアを個別に販売する形式でのライセンシングではなく、より自由な流通形態とソフトウェア権利者保護を目的とした新たな流通方法が提案されている。このような流通方法の典型的な例としては、文献（森亮一、田代秀一「ソフトウェア・サービス・システム（ＳＳＳ）の提案」電子情報通信学会論文誌 '８７／１　Ｖｏｌ．Ｊ７０－Ｄ　Ｎｏ．１）が知られている。
【０００５】この文献には、“ソフトウェアサービスシステム（ＳＳＳ）”と称されるソフトウェア流通システムが紹介されている。ＳＳＳでは、暗号化されたソフトウェア本体とそれを解読するための機能を持つヘッダ部とから構成されるソフトウェア構造が利用される。また、“共通クレジット”と“許諾条件プログラム”という２つの概念を利用して、ユーザとソフトウェア権利者間のライセンシングとソフトウェア使用料の管理が行われている。
【０００６】“共通クレジット”は、量的にどれだけのソフトウェアの使用をユーザに許すかという情報が記憶されたＩＣカードなどから構成されるものである。ＳＳＳによって配布されたソフトウェアを使用したいと考えるユーザは、まず、ＳＳＳのサービスセンタに行って適当な料金を支払い、その額に対応する情報が書き込まれた共通クレジットを受け取る。
【０００７】“許諾条件プログラム”は、共通クレジットに書き込まれた情報の値からユーザの契約残高を認識し、ソフトウェアを実行を許可またき禁止するためのプログラムである。この許諾条件プログラムは、ある値以上の共通クレジットが計算機上に存在することを確認した上でソフトウェアが実行を許し、そしてそのソフトウェアの価値に応じた量だけ共通クレジットの値（契約残高に相当する）をデクリメントする。
【０００８】しかしながら、このような共通クレジットを使用したソフトウェア使用料の管理方法では、共通クレジットの複製やそのデータ書き替えに対する保護が必要とされ、そのために、例えば共通クレジットのリード／ライトを制限するための専用のハードウェア機構などが必要となるという問題がある。
【０００９】
【発明が解決しようとする課題】そこで、最近では、暗号化されたソフトウェアをユーザに無償または低価格で配布しておき、ユーザが使用を希望するソフトウェアを復号化するためのキーを使用料と引き換えにユーザに発

行するというソフトウェア流通システムが提案され始めている。

【００１０】このような流通システムを採用することによって、ソフトウェアベンダは個別のソフトウェアのパッケージ作成および流通にかかるコストを節約できるほか、暗号化されたソフトウェアの内容を紹介するためのデモンストレーション版をＣＤ－ＲＯＭなどの媒体に一緒にパッケージングしておくことにより、その媒体をソフトウェアの有効な宣伝手段として用いることができる。また、ユーザから見ると、ソフトウェアの正式な購入前にそのソフトウェアが購入に値するかどうかを試用によって確認できるという利点がある。

【００１１】ユーザは、希望するソフトウェアの使用料の支払いと引き換えに復号キーを受け取り、その受け取ったキーを使って自分の計算機のハードディスクにソフトウェアの正式版をインストールする。

【００１２】このように、復号キーを利用したソフトウェア流通システムは、その復号キーの受け渡しによってソフトウェア使用料の管理を行えるため、ＳＳＳのような共通クレジットやそれを管理するための専用のハードウェアが不要となり、より自由度の高い流通形態を実現できる。

【００１３】ところで、ユーザによるコンピュータの通常の使用形態を考えると、ハードディスクの空き容量を増やすためにインストール済みのソフトウェアを一旦消去し、後日必要になった時に再インストールするということが頻繁に行われている。暗号化されてない通常のパッケージソフトウェアの場合には、パッケージに含まれている記録媒体自体はユーザの手元に残っているので、ハードディスク上にインストールされたソフトウェア自体は消えてしまっても構わない。後日そのソフトウェアが必要になった場合は、あらためて記録媒体からのインストールが可能だからである。

【００１４】これに対して、前述したような復号キーを利用したソフトウェア流通システムの場合には、ユーザの手元に残っているの実行可能なソフトウェアは、復号キーを利用して復号化されたハードディスク上のソフトウェアでけである。したがって、もしユーザがソフトウェアベンダから利用料と引き替えに入手した復号キーを紛失した場合、そのソフトウェアを再インストールする場合には、同じソフトウェアの使用料を再び支払って復号キーを入手しなければならない。このことは、暗号化を利用したソフトウェア流通システムの信頼性を低下させ、その流通システムの普及を妨げる要因となる。

【００１５】この発明はこのような点に鑑みてなされたものであり、暗号化を利用したソフトウェア流通システムにおけるキー管理を改善して、一旦正当な手順で復号化されたソフトウェアについてはソフトウェアベンダからキーを入手しなくても再インストールできるようにし、ソフトウェアの消去および再インストールを自由に行う事が可能な復号鍵管理方法を提供することを目的とする。

【００１６】

【課題を解決するための手段】この発明による復号鍵管理方法は、暗号化されたソフトウェアを導入すべきコンピュータの記憶装置から前記ソフトウェアを解読するための復号鍵を検索し、前記復号鍵を検索できたとき、その復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入し、前記復号鍵を検索できなかったとき、前記暗号化されたソフトウェアの配布元から、前記ソフトウェアに対応する復号鍵を入手するための手続きを実行し、その入手した復号鍵を利用して前記暗号化されたソフトウェアを復号化して前記コンピュータの記憶装置に導入すると共に、その復号鍵を前記ソフトウェアと別個に前記コンピュータの記憶装置内に保存し、前記暗号化されたソフトウェアの再導入のときは前記記憶装置内に保存されている復号鍵を利用して前記ソフトウェアを復号化できるようにしたことを特徴とする。

【００１７】この復号鍵管理方法においては、ソフトウェアの配布元から復号鍵を入手したとき、その復号鍵は、ソフトウェア本体の復号化に利用されると共に、例えば、復号化されたソフトウェア本体と別個のファイルなどとしてコンピュータの記憶装置内に保存される。したがって、復号化されたソフトウェア本体を記憶装置から消去した場合でも、復号鍵は保存されたまま消去されない。したがって、初めてインストールするソフトウェアについてはソフトウェア配布元から復号鍵を入手する手続きが必要となるが、既にインストールされたことのあるソフトウェアを再インストールする場合には記憶装置に保存されている復号鍵によって復号化することができる。よって、一旦正当な手順で復号化されたソフトウェアについてはソフトウェアベンダからキーを入手しなくてもその再インストールを実行できるようになり、ソフトウェアの消去および再インストールを自由に行う事が可能になる。

【００１８】ソフトウェア本体がインストールされる記憶装置と復号鍵が保存される記憶装置は例えば同一のハードディスク装置などであってもよいが、ソフトウェア本体がインストールされる記憶装置とは別に、復号鍵を記憶するための復号鍵記憶装置を用意しても良い。この場合、復号鍵記憶装置には消去されたソフトウェアに対応する復号鍵だけが保存されていれば十分であり、記憶装置に残っているソフトウェアの復号鍵は不要ある。このため、ソフトウェアの配布元から復号鍵を入手したときは、復号鍵はソフトウェア本体がインストールされる記憶装置に格納しておき、そのソフトウェア本体が消去されるときに、そのソフトウェア本体に対応する復号鍵を復号鍵記憶装置に移して保存することが好ましい。

【００１９】また、この発明によるソフトウェアインス

トールの手順は、暗号化ソフトウェアと付随して配布される復号化プログラムに記述しておくことが好ましい。この場合、インストールに必要な全ての手続きが復号化プログラムによって自動的に実行されるので、ユーザは、初めてインストールするもののか、再インストールするものかによらず、使用したいソフトウェア内の復号化プログラムを実行するだけで済む。

【００２０】また、このような復号化プログラムは、配布されるソフトウェア単位では無く、各種暗号化ソフトウェアをコンピュータにインストールするための共通のインストーラとして実現してもよい。この場合、ソフトウェア配布元から入手された復号鍵は、ソフトウェア識別情報と対応付けて保存する事が好ましい。これにより、ソフトウェア識別情報を検索キーとして利用できるようになり、どの暗号化ソフトウェアをインストールする場合でも、それに対応する復号鍵の検索処理を行うことが可能になる。

【００２１】

【発明の実施の形態】以下、図面を参照して、この発明の実施の形態を説明する。図１には、この発明の一実施形態に係るソフトウェア流通システム全体の構成が示されている。

【００２２】このソフトウェア流通システムは、暗号化されたソフトウェアをユーザに無償または低価格で配布しておき、ソフトウェア使用料の支払いと引き換えにユーザが使用を希望するソフトウェアを復号化するための復号キーを発行するというソフトウェア流通方法を実現するためのものであり、複数の加入ユーザ端末とソフトウェアベンダ、およびそれらを繋ぐ通信網から構成される。ここで、暗号化されたソフトウェアとは、暗号化されたプログラム、暗号化されたデータなどを意味する。

【００２３】図１においては、加入ユーザ端末としてパーソナルコンピュータ１１が代表して示されており、そのパーソナルコンピュータ１１は、電話回線やＩＳＤＮなどの通信網１５を介してソフトウェアベンダ１４に設置された計算機センタに接続されている。

【００２４】ソフトウェアベンダ１４は、暗号化された複数のソフトウェアと、それらソフトウェアの内容を紹介するためのデモンストレーション版ソフトなどが一緒に収容されたＣＤ－ＲＯＭ１０などの大容量記録媒体を通じて、無償または低価格でユーザに配布する。また、ソフトウェアベンダ１４は、配布した暗号化ソフトウェアそれぞれについて、それを復号化するための復号キーを保持および管理している。

【００２５】ＣＤ－ＲＯＭ１０に記録された１つのソフトウェアは、インストーラ１０１、ソフトウェア識別情報（ＩＤ）１０２、およびソフトウェア本体１０３から構成されている。この場合、ソフトウェア本体１０３は暗号化されているが、インストーラ１０１およびソフトウェア識別情報（ＩＤ）１０２については暗号化はされていない。また、デモンストレーション版についても、暗号化はなされていない。

【００２６】インストーラ１０１は、暗号化されたソフトウェア本体１０３を復号化してユーザの使用するパーソナルコンピュータ１１にインストールするためのプログラムである。ソフトウェア識別情報（ＩＤ）１０２は、暗号化されたソフトウェアを特定するための固有のＩＤである。ソフトウェア本体１０３は、所定のオペレーティングシステム下で動作するアプリケーションプログラムやユーティリティプログラム、あるいは画像情報などの各種データファイルなどである。

【００２７】パーソナルコンピュータ１１の２次記憶装置として使用されるハードディスク装置１２には、パーソナルコンピュータ１１で実行されるオペレーティングシステムや各種アプリケーションプログラム、または各種データファイルがインストールされている。また、このハードディスク装置１２の記憶領域には、復号キー記憶部１３が用意されている。

【００２８】復号キー記憶部１３は、インストーラ１０１によって参照可能な独立した１種のデータファイルであり、一度インストールされた暗号化ソフトウェアそれぞれについてそのソフトウェアＩＤと、そのソフトウェアを復号化するためにソフトウェアベンダ１４から入手した復号キーとが対応付けられて保存されている。この復号キー記憶部１３の復号キーは、再インストールされる暗号化ソフトウェアを復号化するために利用される。

【００２９】復号キー記憶部１３へのソフトウェアＩＤおよび復号キーの保存は、ソフトウェアベンダ１４から復号キーを入手したときに行われる。また、実際には、復号キー記憶部１３には消去されたソフトウェアに対応する復号鍵だけが保存されていれば十分であるので、ソフトウェア本体１０３がが消去されるときに、それに対応するソフトウェアＩＤおよび復号キーを復号キー記憶部１３に保存しても良い。

【００３０】図２には、インストーラ１０１のプログラム構造が示されている。インストーラ１０１は、図２に示されているように、復号キー検索プログラム、通信プログラム、復号およびインストールプログラム、および復号キー保存プログラムを含んでいる。以下、これらプログラムによって実行される機能を図３を参照して説明する。

【００３１】復号キー検索プログラムは、復号キー記憶部１３を検索して、暗号化されたソフトウェア本体１０３を復号化するための復号キーを取得する。前述したように、復号キー記憶部１３には、既にインストールされた暗号化ソフトウェアに対応するソフトウェアＩＤと復号キーとが登録されている。このため、復号キー検索プログラムによる復号キー検索は、ソフトウェア識別情報（ＩＤ）１０２と復号キー記憶部１３のソフトウェアＩＤとを順次比較する順次検索、あるいは２分検索などに

よって行われる。

【００３２】通信プログラムは、ソフトウェア使用料の支払いとの引き換えにソフトウェアベンタ１４から復号キーを入手するために、通信回線１５を介してソフトウェアベンタ１４と通信する。この通信プログラムには、復号キー要求メッセージをソフトウェアベンタ１４に送信するルーチンと、ソフトウェアベンタ１４から復号キーを受信するルーチンが含まれている。この通信プログラムは、復号キー検索プログラムによる復号キー検索が失敗した時、つまり該当する復号キーが復号キー記憶部１３に存在しなかったときに実行される。

【００３３】復号およびインストールプログラムは、復号キー検索プログラムによるキー検索が成功した場合にはそのキーを、失敗した場合には通信プログラムによってソフトウェアベンタ１４から入手されたキーを使用して、ソフトウェア本体１０３を復号化し、ハードディスク装置１２にインストールする。

【００３４】復号キー保存プログラムは、通信プログラムによってソフトウェアベンタ１４から入手された復号キーを、ソフトウェアＩＤと対応付けて復号キー記憶部１３に保存する。

【００３５】このように構造を持つインストーラ１０１によれば、ソフトウェアベンダ１４から復号キーを入手したときに、その復号キーは、ソフトウェア本体１０３の復号化に利用されると共に、その復号化されたソフトウェア本体１０３とは別個のファイルとしてに復号キー記憶部１３に保存される。このため、復号化されたソフトウェア本体をハードディスク装置１２から消去しても復号キーについては消去されずに復号キー記憶部１３に保存されたまま維持される。

【００３６】したがって、既にインストールされたことのあるソフトウェアを再インストールする場合には、復号キー記憶部１３に保存されている復号キーを利用することによりそれを直ちに復号化することができる。また、初めてインストールする暗号化ソフトウェアについては、インストーラ１０１によって自動的にベンダ１４から復号キーを入手することができる。

【００３７】次に、図４を参照して、通信プログラムによってソフトウェアベンダ１４に送信される復号キー要求メッセージのデータ構造について説明する。復号キー要求メッセージには、図示のように、通信に必要な情報を含むヘッダ部２１に加え、パーソナルコンピュータ１１のマシンＩＤ２２、インストール対象の暗号化ソフトウェアのソフトウェアＩＤ２３、ユーザ名２４、およびユーザのクレジット番号などが含まれている。

【００３８】次に、図５を参照して、復号キー要求メッセージを受信した場合におけるソフトウェアベンダ１４の動作を説明する。ソフトウェアベンダ１４は、復号キー要求メッセージからソフトウェアＩＤを検出し、ユーザが希望しているソフトウェアを特定する。そして、そのソフトウェアに対応する使用料金、ユーザ名、クレジッシ番号などから課金処理のために必要な情報を生成し、自らまたはクレジット会社などに委託して課金処理を行う。。この後、ソフトウェアベンダ１４は、ソフトウェアＩＤに対応する復号キーを、復号キー要求メッセージ発行元のユーザに送信する。この場合、復号キーはユーザのマシンＩＤを用いて暗号化して送り、インストーラ２０１がそれをマシンＩＤを用いて復号化してから使用するという運用形態を利用する事もできる。

【００３９】このように、復号化キーの要求および発行によってソフトウェア使用料の管理が自動的に行われる。図６には、インストーラ１０１の機能をパーソナルコンピュータ１１に組み込んでおき、それを各種暗号化ソフトウェアをコンピュータ１１にインストールするための共通のインストーラとして利用する場合の例が示されている。

【００４０】すなわち、図６のパーソナルコンピュータ１１には復号キー管理システム５１が設けられており、この復号キー管理システム５１は複数の暗号化ソフトウェアの共通インストーラとして機能として利用される。復号キー管理システム５１は、この発明の流通システムを実現するために各ユーザのパーソナルコンピュータ１１にインストールされて使用されるプログラムとして実現する事ができる。

【００４１】この場合、復号キー管理システム５１には、図２に示したインストーラ１０１と同様のプログラム群、すなわち、復号キー検索プログラム、通信プログラム、復号およびインストールプログラム、および復号キー保存プログラムから構成できる。

【００４２】このような復号キー管理システム５１を利用する場合には、暗号化ソフトウェアには、ソフトウェア本体とソフトウェアＩＤが登録されていれば良く、インストーラは不用である。各暗号化ソフトウェアのソフトウェアＩＤは、復号キー記憶部１３の検索に利用される。

【００４３】次に、図７乃至図９を参照して、図１のソフトウェア流通システムにおける復号キー管理処理の手順を具体的に説明する。図７には、図１のソフトウェア流通システムの運用形態の一例が示されている。ここでは、図１のハードディスク装置１２に対応する記憶装置として、復号キー記憶部兼ソフトウェア本体記憶部６１が使用されている。図中の破線は、ソフトウェア識別子（ＩＤ）および復号キーのみが復号キー記憶部兼ソフトウェア本体記憶部６１に記憶されており、ソフトウェア本体は消去されて記憶されていない状態を表している。

【００４４】ソフトウェア本体入手部６２が通信回線や図１のＣＤ－ＲＯＭ１０などの記憶媒体の購入などの手段によってソフトウェアベンダ１４から入手した暗号化ソフトウェアをユーザのパーソナルコンピュータ１１にインストールする際には、復号キー入手部６３は、その

ソフトウェアのソフトウェアＩＤを検索のキーとして使用して、復号キー記憶部兼ソフトウェア本体記憶部６１からそのソフトウェアの復号キーを検索する。復号キー入手部６３は、前述したインストーラ１０１または復号キー管理システム５１の復号キー検索プログラム、通信プログラム、おわび復号キー保存プログラムに相当している。

【００４５】見つかった場合はその復号キーを利用するが、見つからなかった場合は、復号キー入手部６３がソフトウェアベンダ１４等から復号キーを通信回線・記憶媒体の購入などの手段によって入手し、ソフトウェアＩＤと復号キーを対応付けて復号キー記憶部兼ソフトウェア本体記憶部６１に格納する。そして、ソフトウェア本体入手部６２によってソフトウェア本体が復号化され、復号キー記憶部兼ソフトウェア本体記憶部６１にインストールされる。ソフトウェア本体入手部６２は、前述したインストーラ１０１または復号キー管理システム５１の復号およびインストールプログラムに相当している。

【００４６】あるソフトウェア本体を消去する際には、復号キー保存部６４によってソフトウェア本体のみが消去され、ソフトウェアＩＤおよび復号キーはそのまま復号キー記憶部兼ソフトウェア本体記憶部６１内に保存される。これは、ソフトウェアＩＤと復号キーとの組みをソフトウェア本体と別個に記憶しておくことなどによって実現できるものである。

【００４７】また、復号キー保存部６４は、ソフトウェア本体を消去するという点で、ファイル管理システムとして実現できる。この場合、復号キー保存部６４は、ユーザからのプログラムファイル消去命令に応じて該当するソフトウェア本体だけを削除することになる。また、ファイル消去命令に応じて、消去対象のソフトウェア本体に対応するソフトウェアＩＤおよび復号キーを復号キー記憶部兼ソフトウェア本体記憶部６１から読み取っておき、ソフトウェア本体の消去後に、読み取ったソフトウェアＩＤおよび復号キーを復号キー記憶部兼ソフトウェア本体記憶部６１に書き戻すといった処理を行ってもよい。

【００４８】このようにして、復号キー保存部６４により、ソフトウェアＩＤおよび復号キーはソフトウェア本体が消去されても復号キー記憶部兼ソフトウェア本体記憶部６１にそのまま維持される。

【００４９】図７の復号キー記憶部兼ソフトウェア本体記憶部６１では、ソフトウェア１，…，ｎがインストールされ、そのうちソフトウェア２，ｎなどのソフトウェア本体が消去されているが、ソフトウェア識別子および復号キーはそれらのソフトウェアを含めて１，…，ｎすべてについて保存されている。

【００５０】なお、このように復号キー記憶部とソフトウェア本体記憶部と兼ねることにより、保存の処理が簡易であるほか、ハードディスクなどのソフトウェア本体記憶部以外には他の外部記憶装置が不要であるという利点がある。

【００５１】図８には、図１のソフトウェア流通システムの他の運用形態の一例が示されている。ここでは、ソフトウェア本体記憶部７１は図１のハードディスク装置１２に相当し、これとは別の記憶装置として復号キー記憶部７５が設けられている。

【００５２】ソフトウェア本体入手部７２が通信回線や記憶媒体の購入などの手段によってソフトウェアベンダ１４から入手した暗号化ソフトウェアをインストールする際には、まずそのソフトウェアＩＤを検索のキーとして復号キー入手部７３が復号キー記憶部７５からそのソフトウェアの復号キーを検索する。復号キー入手部７３は、前述したインストーラ１０１または復号キー管理システム５１の復号キー検索プログラム、通信プログラム、および復号キー保存プログラムに相当している。

【００５３】見つかった場合はその復号キーを利用するが、見つからなかった場合は、復号キー入手部７３がソフトウェアベンダ１４等から復号キーを通信回線・記憶媒体の購入などの手段によって入手し、ソフトウェアＩＤと復号キーをソフトウェア本体記憶部７１に格納する。そして、ソフトウェア本体入手部７２によってソフトウェア本体が復号化され、ソフトウェア本体記憶部７１にインストールされる。ソフトウェア本体入手部７２は、前述したインストーラ１０１または復号キー管理システム５１の復号およびインストールプログラムに相当している。

【００５４】あるソフトウェア本体を消去する際には、復号キー保存部７４によってソフトウェア識別子・復号キー・ソフトウェア本体がソフトウェア本体記憶部７１から消去され、ソフトウェアＩＤおよび復号キーが復号キー記憶部７５に保存される。すなわち、復号キー保存部７４は一種のファイル管理システムでもあり、削除対象のソフトウェア本体に対応するソフトウェアＩＤおよび復号キーをソフトウェア本体記憶部７１から取り出して、それを復号キー記憶部７５に保存する。このため、復号キー記憶部７５には、ソフトウェア本体記憶部７１から削除されたソフトウェア本体に対応するソフトウェアＩＤおよび復号キーだけが保存されることになり、ソフトウェア本体記憶部７１に残っているソフトウェア本体に対応するソフトウェアＩＤおよび復号キーについては保存されない。よって、復号キー記憶部７５に不要な情報（消去されてないソフトウェア本体のソフトウェアＩＤおよび復号キー）が保存されることがなくなり、検索効率の向上などを図ることができる。

【００５５】図８の例では、ソフトウェア本体記憶部はソフトウェア１，…，ｎがインストールされていたが、そのうち２，ｎなどのソフトウェア本体が消去されたため、それらのソフトウェアのソフトウェアＩＤおよび復号キーもソフトウェア本体記憶部７１から消去されてい

る。これらの消去されたソフトウェアのソフトウェアＩＤおよび復号キーは復号キー記憶部７５に格納されている。

【００５６】ここでは、ソフトウェアＩＤおよび復号キーをソフトウェア本体とは別の記録媒体に記憶することによって、災害などによってソフトウェア本体を記録した媒体が障害を受け、ソフトウェア本体が失われた場合でも、ソフトウェアＩＤおよび復号キーは失われないという利点がある。

【００５７】また、この媒体としてフロッピーディスクなどの取り外し可能な媒体を利用することによって、他の計算機にソフトウェアをインストールすることもできる。この場合には、前述したマシンＩＤによる復号キーの暗号化は行われないものとする。

【００５８】図９には、暗号化ソフトウェアのインストール処理の手順が示されている。ここでは、暗号化ソフトウェアと一緒に配布されるインストーラ１０１を使用してインストールする場合を例にとって説明する。

【００５９】ユーザによって実行が指示されると、まず、インストーラ１０１の復号キー検索プログラムが起動され、復号キー記憶部（図１の復号キー記憶部１３、図７の復号キー記憶部兼ソフトウェア本体記憶部６１、または図８の復号キー記憶部７５）から該当するソフトウェア本体の復号キーを検索し、復号キー記憶部に復号キーが存在するか否かを調べる（ステップＳ１１）。

【００６０】復号キー記憶部に目的とする復号キーが存在しなかったならば、通信プログラムが実行され、復号キー入手処理が行われる（ステップＳ１２）。すなわち、図２のようにデータ構造を持つ復号キー要求メッセージが通信回線を介してユーザのパーソナルコンピュータからソフトウェアベンダに送られ、そこで使用料支払いのための手続きが行われる。この後、復号キーが通信回線を介してソフトウェアベンダからユーザのパーソナルコンピュータに送られる。なお、ユーザのパーソナルコンピュータが通信回線に接続されてない場合には、通信プログラムは復号キーを入手する必要がある旨のメッセージやソフトウェアベンダの電話番号などを画面表示して、ユーザに対して復号キーの入手を促せばよい。

【００６１】ソフトウェアベンダから入手された復号キーは、復号キー保存プログラムによってソフトウェアＩＤと対応付けられて復号キー記憶部（図１の復号キー記憶部１３、図７の復号キー記憶部兼ソフトウェア本体記憶部６１、または図８のソフトウェア本体記憶部７１）に格納される（ステップＳ１３）。

【００６２】この後、入手した復号化キーによってソフトウェア本体が復号化され（ステップＳ１４）、記憶装置（図１のハードディスク装置１２、図７の復号キー記憶部兼ソフトウェア本体記憶部６１、または図８のソフトウェア本体記憶部７１）にインストールされる（ステップＳ１５）。

【００６３】一方、復号キー記憶部に目的とする復号キーが存在したならば、ステップＳ１２、Ｓ１３の処理は行われず、復号キー記憶部に保存されている復号キーが利用されて、ソフトウェア本体の復号化処理（ステップＳ１４）、およびインストール処理（ステップＳ１５）が実行される。

【００６４】なお、以上の説明では、復号キーは常にソフトウェアＩＤと対応付けて保存するように説明したが、暗号化ソフトウェアと一緒に配布されるインストーラ１０１を使用してインストールする場合には、復号キーを１つのファイルとして保存し、そのファイル名としてソフトウェアＩＤを利用することともできる。

【００６５】

【発明の効果】以上説明したように、この発明によれば、ソフトウェアの識別子とソフトウェアを復号化するためのキーとが保存され、次回にそのソフトウェア本体を再び復号化する際にはそのキーが再利用されるため、利用者は復号キーを複数回入手せずに済む。よって、ソフトウェアの消去および再インストールを自由に行う事が可能になり、暗号化を利用したソフトウェア流通システムの信頼性の向上を図ることができ、その流通システムの普及に寄与することができる。

【図面の簡単な説明】

【図１】この発明の一実施形態に係るソフトウェア流通システム全体の構成を示すブロック図。

【図２】同実施形態に係るソフトウェア流通システムで配布される暗号化ソフトウェアに付随するインストーラのプログラム構造の一例を示す図。

【図３】図２のインストーラの機能を説明するための図。

【図４】同実施形態に係るソフトウェア流通システムにおいてユーザ端末からソフトウェアベンダに送信される復号キー要求メッセージのデータ構造の一例を示す図。

【図５】同実施形態に係るソフトウェア流通システムにおけるソフトウェアベンダの機能を説明するための図。

【図６】同実施形態に係るソフトウェア流通システムのユーザ端末に設けられる復号キー管理システムの機能を説明するための図。

【図７】同実施形態に係るソフトウェア流通システムの運用形態の一例を概念的に示す図。

【図８】同実施形態に係るソフトウェア流通システムの運用形態の他の例を概念的に示す図。

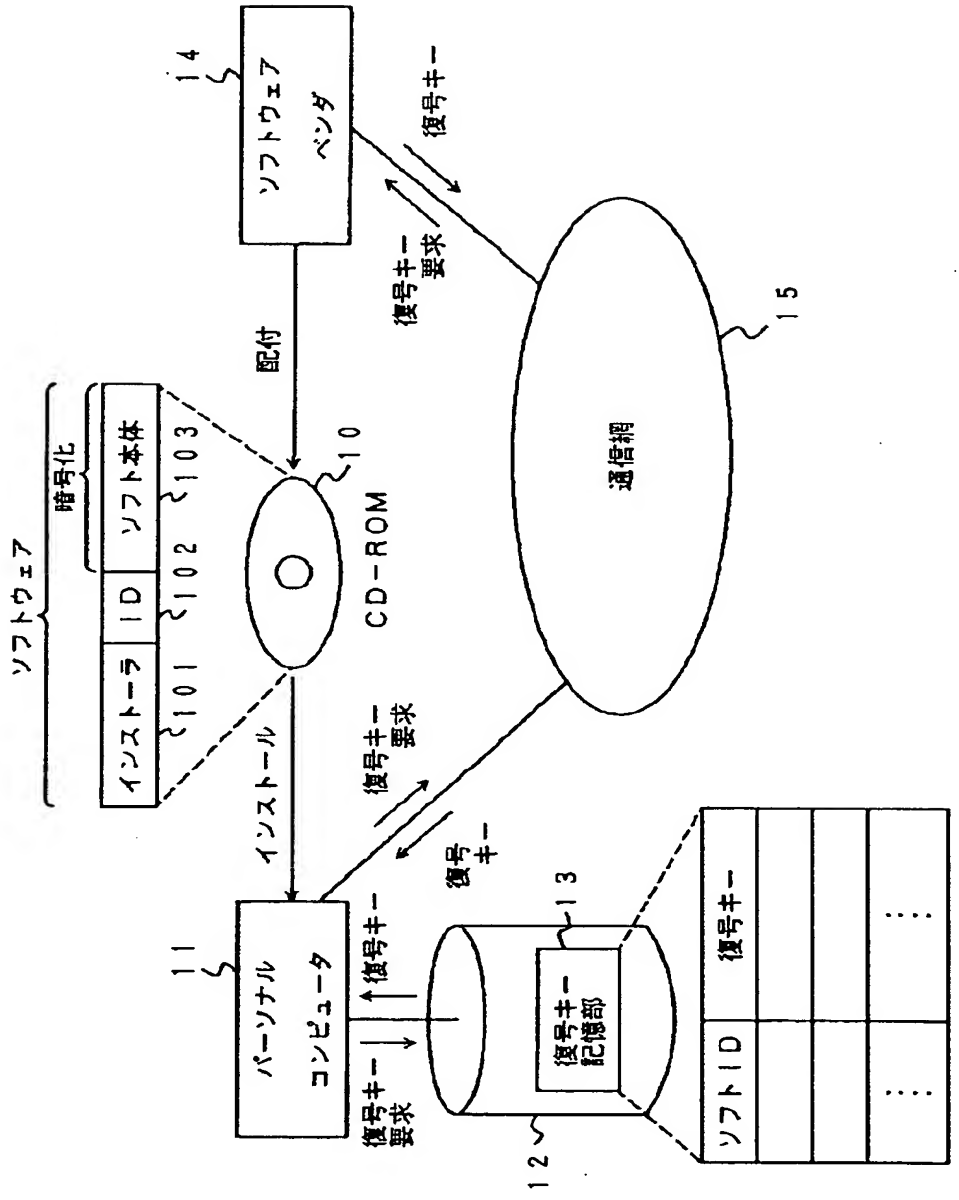
【図９】同実施形態に係るソフトウェア流通システムにおける暗号化ソフトウェアのインストール手順を説明するためのフローチャート。

【符号の説明】

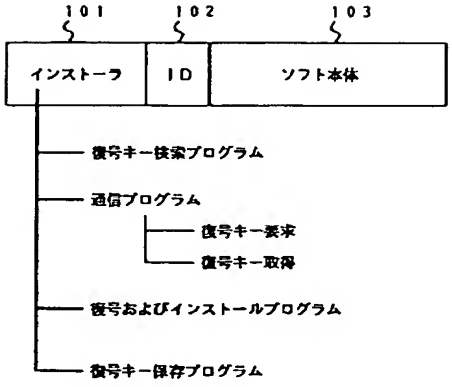
１１…パーソナルコンピュータ（ユーザ端末）、１２…ハードディス装置、１３，７５…復号キー記憶部、１４…ソフトウェアベンダ、１５…通信網、５１…復号キー管理システム、６１…復号キー記憶部兼ソフトウェア本

体記憶部、６２，７２…ソフトウェア本体入手部、６３，７３…復号キー入手部、６４，７４…復号キー保存部、７１…ソフトウェア本体記憶部、１０１…インストーラ、１０２…ソフトウェアＩＤ、１０３…ソフトウェア本体。

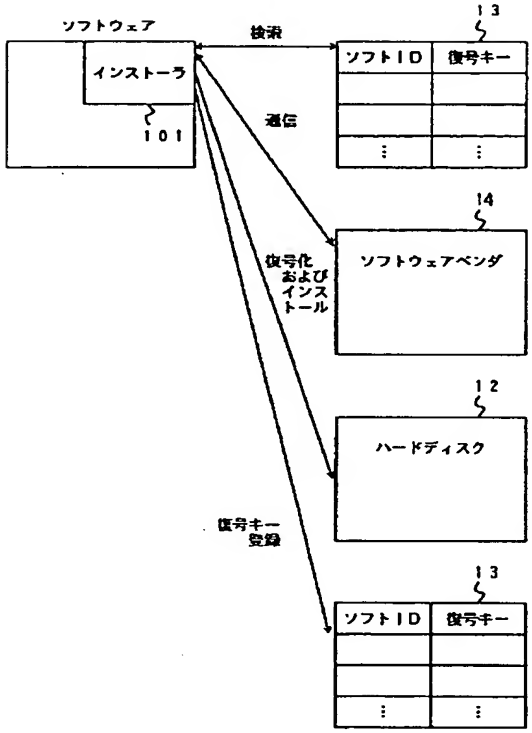
【図１】



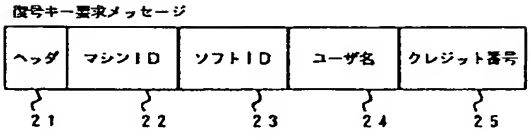
【図２】


101
102
103
インストーラ
ID
ソフト本体
復号キー検索プログラム
通信プログラム
復号キー要求
復号キー取得
復号およびインストールプログラム
復号キー保存プログラム

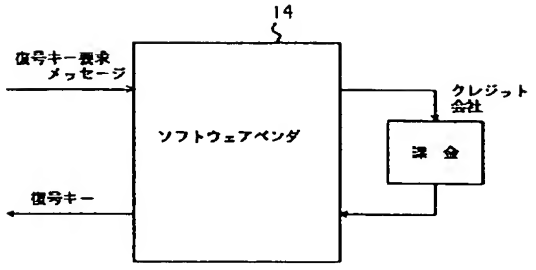
【図３】


ソフトウェア
インストーラ
101
検索
通信
復号化およびインストール
復号キー登録
13
ソフトID
復号キー
14
ソフトウェアベンダ
12
ハードディスク
13
ソフトID
復号キー

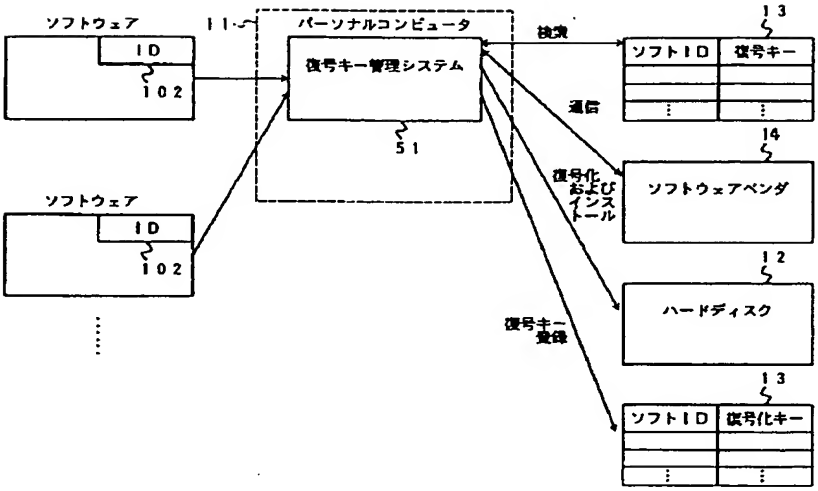
【図４】


復号キー要求メッセージ
ヘッダ
マシンID
ソフトID
ユーザ名
クレジット番号
21
22
23
24
25

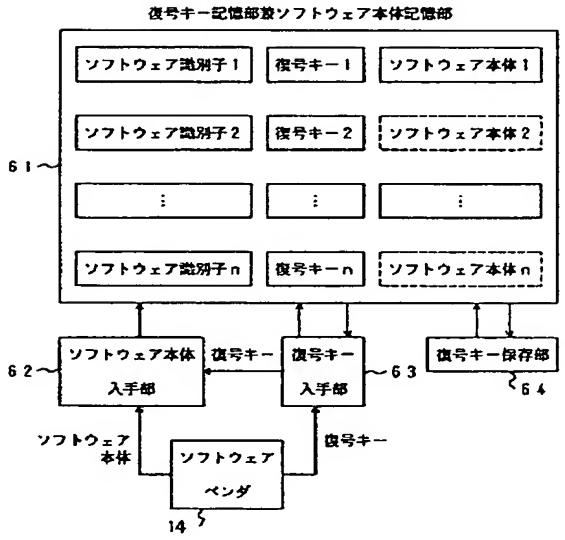
【図５】


14
復号キー要求メッセージ
ソフトウェアベンダ
クレジット会社
課 金
復号キー

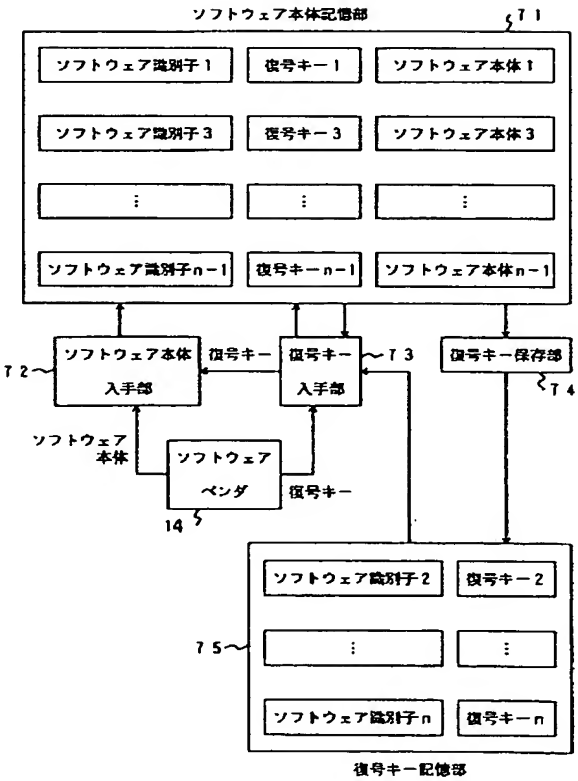
【図６】


ソフトウェア
ID
102
ソフトウェア
ID
102
11
パーソナルコンピュータ
復号キー管理システム
51
検索
通信
復号化およびインストール
復号キー登録
13
ソフトID
復号キー
14
ソフトウェアベンダ
12
ハードディスク
13
ソフトID
復号化キー

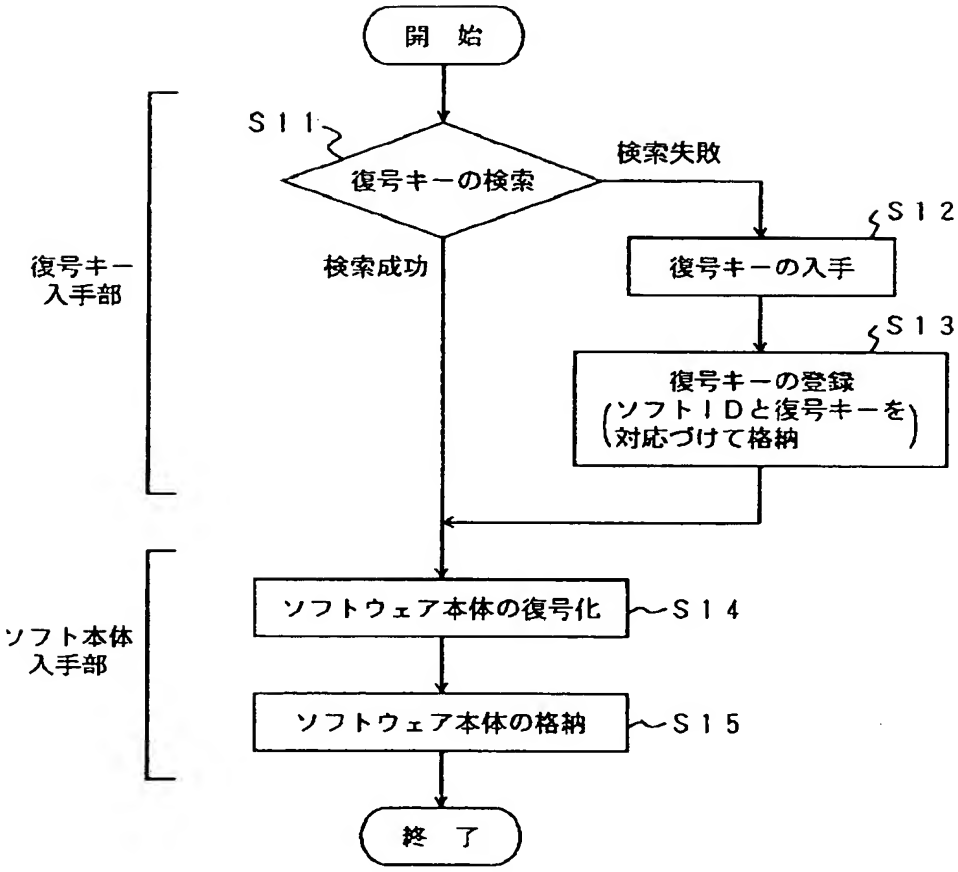
【図７】


復号キー記憶部及ソフトウェア本体記憶部
ソフトウェア識別子1
復号キー1
ソフトウェア本体1
ソフトウェア識別子2
復号キー2
ソフトウェア本体2
ソフトウェア識別子n
復号キーn
ソフトウェア本体n
61
ソフトウェア本体入手部
復号キー
復号キー入手部
63
復号キー保存部
64
62
ソフトウェア本体
ソフトウェアベンダ
復号キー
14

【図８】


ソフトウェア本体記憶部
71
ソフトウェア識別子1
復号キー1
ソフトウェア本体1
ソフトウェア識別子3
復号キー3
ソフトウェア本体3
ソフトウェア識別子n-1
復号キーn-1
ソフトウェア本体n-1
72
ソフトウェア本体入手部
復号キー
復号キー入手部
73
復号キー保存部
74
ソフトウェア本体
ソフトウェアベンダ
復号キー
14
75
ソフトウェア識別子2
復号キー2
ソフトウェア識別子n
復号キーn
復号キー記憶部

【図９】


開　始
Ｓ１１
復号キーの検索
検索失敗
検索成功
Ｓ１２
復号キーの入手
Ｓ１３
復号キーの登録
(ソフトＩＤと復号キーを
対応づけて格納)
復号キー
入手部
ソフトウェア本体の復号化
Ｓ１４
ソフトウェア本体の格納
Ｓ１５
ソフト本体
入手部
終　了